Berlin, 03.07.2025

Stellungnahme und Kommentierung

zum

Referentenentwurf des Bundesministeriums des Innern für ein Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

Kontakt:
RA Karsten U. Bartels, LL.M.
HK2 RAe
Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Stellvertretender Vorstandsvorsitzender
Leiter TeleTrusT-AG "IT-Sicherheitsrecht"
bartels@hk2.eu

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Fachleute, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Personenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany" und "IT Security made in EU". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4310
https://www.teletrust.de

I. Allgemeine Vorbemerkung

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) hält die Ausweitung der Regulierung gesetzlicher IT-Sicherheit in Deutschland und der EU für dringender denn je. Das betrifft die Verbreiterung der KRITIS-Regulierung durch die NIS-2-Richtlinie, die Umsetzung der CER-Richtlinie sowie auch die horizontale Regulierung durch den EU Cyber Resilience Act.

Anlass dafür ist die historisch schlechte IT-Sicherheitslage, die weitere Zunahme der Bedrohungen sowie die mangelnde freiwillige Umsetzung von hinreichender IT-Sicherheit in Unternehmen und Verwaltung.

TeleTrusT ist es ein besonderes Anliegen, dass das NIS-2-Umsetzungsgesetz handwerklich und systematisch präzise gestaltet wird. Durch die mangelnde Umsetzungsfrist ist es von besonderer Bedeutung, dass das Gesetz aus sich heraus funktional, widerspruchsfrei und anwendbar ist. Auf die seit dem 17.10.2024 verstrichene Frist und das EU-Vertragsverletzungsverfahren wird hingewiesen. TeleTrusT besorgt insbesondere § 28 Abs. 3 BSIG-E, der auch mit der Neuformulierung in diesem Referentenentwurf allenfalls noch als problematisch bezeichnet werden kann. Die Europarechtswidrigkeit liegt nahe.

II. Anmerkungen zu ausgewählten Regelungen des BSIG-E

1. § 6 BSIG-E, Informationsaustausch

TeleTrusT kritisiert § 6 BSIG-E: es ist aus Sicht der IT-Sicherheit wünschenswert, dass sämtliche Interessierten an die in der Norm genannten Informationen gelangen, nicht nur die Betreiber wichtiger und besonders wichtiger Einrichtungen, Einrichtungen der Bundesverwaltung sowie die Hersteller, Dienstleister und Lieferanten. Zwar ist vorgesehen, auch weiteren Stellen eine Teilnahme zu ermöglichen. Diese Kann-Regelung geht jedoch am Informationsinteresse der Öffentlichkeit und der Unternehmen vorbei. Es ist kein belastbarer Grund erkennbar, die betreffenden Informationen nicht schlicht zu veröffentlichen. Zumal es keinerlei Handhabe gibt, eine Weitergabe der Information durch Berechtigte zu verhindern.

Es sollte endlich davon Abstand genommen werden, den Informationszugang weiterhin "mitgliedschaftlich" zu organisieren, wie dies derzeit noch im Rahmen der Allianz für Cybersicherheit umgesetzt wird. So sind Teilnahmebedingungen inklusive einer Geheimhaltungsverpflichtung bislang Voraussetzung für die Informationsteilhabe bei der Allianz für Cybersicherheit.

In § 6 Abs. 2 BSIG-E sind nun ebenfalls Teilnahmebedingungen vorgesehen. TeleTrusT bezweifelt die Zulässigkeit und Notwendigkeit solcher Bedingungen. Sofern nicht im konkreten Einzelfall das Informationsinteresse der Öffentlichkeit aufgrund von Sicherheitsbedenken (durch eine Veröffentlichung) zurückstehen muss, sollte es einen freien Zugang zu den relevanten Informationen für Alle und einen "vorbehaltlosen" Ansatz des BSI geben.

2. § 13 BSIG-E, Warnungen

Der Referentenentwurf enthält eine zu weit gehende Befugnis für Warnungen durch das BSI. Das in § 13 Abs. 1 Ziff. 1 lit. a BSIG-E benannte Tatbestandsmerkmal der "anderen Sicherheitsrisiken in informationstechnischen Produkten und Diensten" wurde nicht definiert und ist unklar. Die Formulierung deutet daraufhin, dass hier ein allgemeiner Auffangtatbestand geschaffen werden soll. Dies lehnt TeleTrusT ausdrücklich ab. Es sollte im Sinne des Bestimmtheitserfordernisses eng umrissen sein, unter welchen Voraussetzungen eine Warnung vorgenommen werden darf. Die Vergangenheit zeigt, dass der Tatbestand politisch motivierte Warnungen nicht ermöglichen darf.

Zudem berechtigt die Norm das BSI, die Öffentlichkeit über "Verstöße besonders wichtiger Einrichtungen oder wichtiger Einrichtungen gegen die Pflichten aus diesem Gesetz" zu informieren. Aufgrund der

Formulierung besteht dieses Recht jedoch bei jeglichem Verstoß gegen eine jegliche Norm des BSIG, unabhängig von der Schwere. Da solche Informationen eine massive Wirkung entfalten können und in geschützte Rechtspositionen der Unternehmen eingegriffen wird, ist eine derart weitgehende und diffuse Rechtsgrundlage abzulehnen.

3. § 15 BSIG-E, Detektion von Angriffsmethoden und von Sicherheitsrisiken für die Netz- und IT-Sicherheit

§ 15 BSIG-E zielt darauf ab, dem BSI die Befugnis zu erteilen, Maßnahmen zur Erkennung von Sicherheitsrisiken und Angriffsmethoden an Schnittstellen öffentlich zugänglicher informationstechnischer Systeme durchzuführen. Diese Befugnisse sind von zentraler Bedeutung für die proaktive Identifizierung und Abwehr von Cyber-Bedrohungen, um die Sicherheit nationaler Netzinfrastrukturen zu gewährleisten. Es wird anerkannt, dass ein solides Verständnis der Bedrohungslandschaft unerlässlich ist, um effektive Schutzmaßnahmen zu entwickeln und die Resilienz kritischer Informationsinfrastrukturen zu stärken.

Allerdings birgt § 15 BSIG-E potenzielle Unzulänglichkeiten in Bezug auf den Schutz von Betriebsgeheimnissen und die Wahrung der Privatsphäre von Nutzern. Es besteht das Risiko, dass die weitreichenden Befugnisse des BSI die grundgesetzlich garantierten Rechte der Bürger und Unternehmen untergraben. Eine Löschung der Informationen ist nur bei Eröffnung des Anwendungsbereichs des Art. 10 GG vorgesehen, § 15 Abs. 1 a. E. BSIG-E. Es ist unklar, wie das Gesetz den notwendigen Schutz der sonstigen grundgesetzlich geschützten Rechte, insbesondere der Persönlichkeitsrechte nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG sicherstellen will.

4. § 18 BSIG-E, Anordnungen von Maßnahmen des Bundesamtes gegenüber Herstellern von IKT-Produkten

Die im § 18 BSIG-E verwendete Formulierung "soweit erforderlich" gibt dem Bundesamt ein weitreichendes Ermessen darüber, wann es von den Herstellern von IKT-Produkten eine Mitwirkung an der Beseitigung oder Vermeidung von Sicherheitsvorfällen verlangt. Hier ist eine Schärfung der Voraussetzung wichtig für eine klare Rechtslage hinsichtlich der Voraussetzungen und Folgen der Norm.

5. §§ 24 ff. BSIG-E, Recht auf Berichtigung und Löschung

Zu § 25 Abs. 1 BSIG-E merken wir an: es ist nicht klar, ob die getroffene Regelung nur für "nicht automatisierte Verarbeitung" gilt, oder auch für die automatisierte Verarbeitung. Es scheint, als ginge der Entwurf davon aus, dass es bei einer automatisierten Verarbeitung stets zu einer Löschung der personenbezogenen Daten kommt, was nicht der Fall sein muss.

In § 24 Abs. 2 BSIG-E ist unklar, was "eine Gegendarstellung" ist, wie eine solche auszugestalten ist und wie das Bundesamt diese Gegendarstellung "den Daten" beifügen würde.

6. §§ 28 ff. BSIG-E, Anwendungsbereich

Grundsätzlich befindet TeleTrusT die Vorschriften zum Anwendungsbereich des BSIG-E für gelungen. Die besonders wichtigen Einrichtungen (mit Ausnahme der Betreiber kritischer Anlagen) und die wichtigen Einrichtungen allein durch die gesetzlichen Regelungen im BSIG-E selbst und deren Anlagen 1 und 2 nachvollziehbar zu machen, schafft Einfachheit und grundsätzlich Rechtssicherheit.

Hinsichtlich der Nomenklatur ist TeleTrusT weiterhin der Ansicht, dass eine Bezeichnung als "wesentliche" und "wichtige" Einrichtungen in Übereinstimmung mit der NIS-2-Richtlinie für EU-weite Einheitlichkeit und damit für Vergleichbarkeit im gemeinsamen Binnenmarkt sorgen würde.

a) Rechtsverordnung (BSI-Kritisverordnung) nach § 56 Abs. 4 BSIG-E

Hinsichtlich dieser Rechtsverordnung nimmt TeleTrusT zur Kenntnis, dass eine Änderung der bestehenden BSI-Kritisverordnung unmittelbar durch den Bundestag geplant ist, vgl. Art. 8 des Entwurfs. Art. 8 und die Begründung zu Art. 8 weisen darauf hin, dass die bisherige BSI-Kritisverordnung übernommen wird und nur vereinzelt Vorschriften angepasst werden sollen.

Die Aufnahme des Sektors "Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitssuchende" ist in Anbetracht der Aufzählung der Sektoren in § 2 Nr. 22 BSIG-E, wo die Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitssuchende eigens aufgeführt sind, konsequent. Inkonsequent erscheint hingegen, bei § 7 Abs. 1 Nr. 5 BSI-Kritisverordnung lediglich die Wörter "Versicherungsdienstleistungen und" zu streichen und damit gerade die Leistungen der Sozialversicherung sowie der Grundsicherung für Arbeitsuchende doppelt zu adressieren. Es ist anzunehmen, dass es sich hierbei um ein Versehen handelt. Die hierzu gehörenden Anlagenkategorien wurden aus Anhang 6 gestrichen. Für den neu eingefügten Sektor sieht Art. 8 jedoch noch keinen eigenen Anhang vor, dies muss so schnell wie möglich eingefügt werden, um als Dienstleister im Bereich Leistungen der Sozialversicherung und Grundsicherung für Arbeitssuchende Rechtsklarheit zu erhalten.

b) § 28 Abs. 3 BSIG-E

Nach § 28 Abs. 3 BSIG-E ist nun nicht mehr bei der Bestimmung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme auf die der Einrichtungsart zuzuordnende Geschäftstätigkeit abzustellen. Die neue Formulierung des § 28 Abs. 3 BSIG-E nimmt dennoch eine Ausnahme vom Anwendungsbereich vor: Hiernach können bei der Zuordnung zu einer der Einrichtungsarten nach den Anlagen 1 und 2 solche Geschäftstätigkeiten unberücksichtigt bleiben, die im Hinblick auf die gesamte Geschäftstätigkeit der Einrichtung vernachlässigbar sind. Die Begründung gleicht dabei der Begründung zu § 28 Abs. 3 Nr. 1 des alten Referentenentwurfs - es soll vermieden werden, dass eine nur geringfügige Nebentätigkeit zu einer unverhältnismäßigen Identifizierung als wichtige oder besonders wichtige Einrichtung führt.

Dabei wird nicht beachtet, dass vom Anwendungsbereich erfasste Einrichtungen aufgrund der Schwellenwerte in der Regel eine bedeutsame Größe aufweisen, die es auch dann rechtfertigen in gesteigerte IT-Sicherheit zu investieren, wenn die Einrichtungsarten nur eine Nebentätigkeit darstellen. Die NIS-2-Richtlinie sieht eine solche Ausnahme ebenfalls nicht vor, sondern folgt einem strikt formellen Einrichtungsbegriff. Die NIS-2-Richtlinie impliziert lediglich in den Erwägungsgründen (Erwägungsgrund 16) eine Ausnahme, wenn die Einrichtung gegenüber ihren Partner- und verbundenen Unternehmen unabhängig ist. Dann können diese bei der Berechnung der Schwellenwerte unberücksichtigt bleiben. Von dieser Ausnahmemöglichkeit macht der Referentenentwurf aber ohnehin in § 28 Abs. 4 BSIG-E Gebrauch. Die darüberhinausgehende Ausnahmeregelung in § 28 Abs. 3 BSIG-E engt den Anwendungsbereich in nicht richtlinienkonformer Weise ein und ist damit europarechtswidrig. Hier besteht dringender Korrekturbedarf.

Unterstellt, die Vorschrift wäre europarechtskonform, wäre sie deutlich zu unbestimmt. Für eine Einordnung einer Geschäftstätigkeit als "vernachlässigbar" bedarf es eindeutiger, objektiver Kriterien.

TeleTrusT wirbt nachdrücklich dafür, möglichst ein-eindeutige Anwendbarkeitsregelungen zu schaffen. Die Aufwände und Rechtsunsicherheit allein im Zusammenhang mit der Rechtsfrage, ob ein Unternehmen unter das Gesetz fällt, werden hier möglicherweise unterschätzt.

c) § 28 Abs. 6 Nr. 1 BSIG-E

Weiterhin unklar bleibt, warum Finanzunternehmen, die in den Anwendungsbereich des Digital Operational Resilience Act ("DORA") fallen, nicht vollständig vom Anwendungsbereich des zukünftigen BSIG ausgenommen werden.

Der DORA ist lex specialis zur NIS-2-Richtlinie, siehe Erwägungsgrund 16 zum DORA sowie Erwägungsgrund 28 zur NIS-2-Richtlinie. Letzterer erwähnt zudem in Satz 3, dass die durch den DORA regulierten Finanzunternehmen auch hinsichtlich Aufsicht und Durchsetzung nicht unter die NIS-2-Richtlinie fallen sollen. Insoweit erscheint es inkonsequent, die in den §§ 61, 62 BSIG-E geregelten Aufsichts- und Durchsetzungsbefugnisse des BSI - im Gegensatz zu den in § 28 Abs. 5 BSIG-E regulierten Unternehmen - auf Finanzunternehmen Anwendung finden zu lassen.

Im Sinne der Rechtssicherheit für die hiervon betroffenen Unternehmen sollten diese insgesamt vom Anwendungsbereich ausgenommen werden.

d) § 29 BSIG-E

Die Aufnahme von Einrichtungen der Bundesverwaltung in den Anwendungsbereich des BSIG-E ist zu begrüßen. Seit dem ersten Referentenentwurf der vergangenen Legislaturperiode hat jedoch eine fortschreitende Aufweichung der adressierten Verwaltungseinrichtungen und der verbundenen Pflichten stattgefunden. Nun werden die weiteren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihre Vereinigungen auf Bundesebene nur noch in Klammern unter § 29 Abs. 1 Nr. 3 aufgeführt, womit deren vollständige Herausnahme aus dem Anwendungsbereich zu befürchten ist. Dies kritisiert TeleTrusT nachdrücklich. Auch die Erklärung der Nichtanwendbarkeit des § 30 BSIG-E auf Einrichtungen der Bundesverwaltung sendet angesichts der desaströsen IT-Sicherheitslage auch im öffentlichen Sektor ein fatales Signal. Dass diese Ausnahme nunmehr in Klammern steht, deutet auf ein Streichen dieser hin, was von TeleTrusT befürwortet werden würde.

Die Geschäftsbereiche des Auswärtigen Amts, der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz sollten ebenfalls umfassend zur IT-Sicherheit verpflichtet werden. Hinsichtlich der vom Auswärtigen Amt zu erlassenden Verwaltungsvorschrift ist bei der Verwendung des Begriffs ("ergebnisäquivalente Maßnahmen") fraglich, ob diese zu einem ausreichenden Maß an IT-Sicherheit verpflichten werden.

e) Anhang 1 und 2 zum BSIG-E

aa) Auslegung des Sektors "Verarbeitendes Gewerbe/Herstellung von Waren", § 28 Abs. 2 BSIG-E

In § 28 Abs. 2 Nr. 3 BSIG-E wird hinsichtlich der anzubietenden Waren und Dienstleistungen auf die Anlagen 1 und 2 verwiesen. Der Sektor erfasst die in den Abteilungen 26 bis 30 NACE genannten wertschöpfenden Tätigkeiten, die im Wesentlichen auf die Herstellung von bestimmten Produkten gerichtet sind. Ob hiervon auch folgende Konstellation erfasst sein soll, geht aus dem Entwurf nicht klar hervor:

Ein Unternehmen stellt ein in den Abteilungen 26 bis 30 NACE aufgeführtes Produkt her, vertreibt dieses jedoch nicht als eigenständiges Produkt, sondern setzt dieses als Werk- bzw. Hilfsmittel oder (Teil-) Komponente ein, um damit das eigentliche Endprodukt herzustellen, das wiederum nicht den Abteilungen 26 bis 30 NACE unterfällt.

Wir gehen davon aus, dass Fälle dieser Art nicht als "entgeltliches Anbieten von Waren oder Dienstleistungen" im Sinne von § 28 Abs. 2 Nr. 3 BSIG-E erfasst sind, weil es für ein Anbieten ausschließlich darauf ankommt, dass das Endprodukt in die Abteilung 26 bis 30 NACE fällt. Anders zu beurteilen wäre dies nur dann, wenn das einer der Abteilungen 26 bis 30 NACE unterfallende Produkt im Rahmen von "Serviceleistungen" etwa eigenständig als Ersatzteil vertrieben werden würde.

Wir empfehlen insoweit eine Klarstellung, zumindest in der Gesetzesbegründung.

bb) Keine Nennung des Teilbereichs ÖPNV im Sektor Transport und Verkehr, Anlage 1

Die aktuelle KRITIS-VO erfasst bestimmte Einrichtungen im Teilbereich ÖPNV im Sektor Transport und Verkehr als Betreiber kritischer Infrastrukturen. Erfasst sind Betreiber von Schienennetzen und Stellwerken sowie Leitzentralen im ÖPSV (siehe Anhang 7 der KRITIS-VO). Demgegenüber erfasst der Sektor Transport und Verkehr in Anlage 1 des BSIG-E aktuell keine Einrichtungen im Teilbereich ÖPNV.

Geht man davon aus, dass solche Einrichtungen in dem Teilbereich ÖPNV auch in Zukunft als Betreiber kritischer Anlagen gemäß der neuen Rechtsverordnung gemäß § 56 Abs. 4 BSIG-E eingestuft werden, führt dies dazu, dass Einrichtungen im Teilbereich ÖPNV so lange nicht vom BSIG-E erfasst werden, wie sie unterhalb der maßgebenden KRITIS-Schwellenwerte liegen. Erst wenn sie die KRITIS-Schwellwerte erreichen und damit als Betreiber kritischer Anlagen eingestuft werden, werden sie dadurch automatisch auch als besonders wichtige Einrichtung eingestuft (vgl. § 28 Abs. 1 Nr. 1 BSIG-E).

Der Kritikalität des Teilbereichs ÖPNV wegen empfehlen wir, diesen ebenfalls in die Anlage 1 aufzunehmen, so dass bei Erreichen der Unternehmenskennzahlen in § 28 Abs. 1 Nr. 4 bzw. Abs. 2 Nr. 3 BSIG-E die entsprechenden Einrichtungen als wichtige bzw. besonders wichtige Einrichtung unabhängig von der Einstufung als Betreiber kritischer Anlagen erfasst werden.

cc) Klarstellung zu "Produktion, Herstellung und Handel mit chemischen Stoffen", Anlage 2

Im Rahmen des Sektors "Produktion, Herstellung und Handel mit chemischen Stoffen" der Anlage 2 Nr. 3 BSIG-E muss klargestellt werden, wer genau dem Anwendungsbereich des Umsetzungsgesetzes unterfallen soll.

Begrüßenswert ist die Klarstellung, dass nur solche Unternehmen adressiert sein sollen, die in die Abteilung 20 NACE Rev. 2 fallen und damit Hersteller von chemischen Erzeugnissen sind. Vor diesem Hintergrund ist davon auszugehen, dass der Verweis auf Art. 3 Nr. 11 der Verordnung (EG) 1907/2006 (Importeure) lediglich ein Redaktionsversehen ist und gelöscht werden kann. Importeure sind im Rahmen von Abteilung 20 NACE Rev. 2 nicht erfasst. Auch würde die Regulierung von Importeuren von den Vorgaben der NIS-2-Richtlinie abweichen, die dies nicht vorsieht.

7. § 30 BSIG-E, Risikomanagementmaßnahmen

Es wäre wünschenswert, die Maßgaben, nach denen die Einrichtungen Maßnahmen zur IT-Sicherheit i. S. v. § 30 Abs. 1 BSIG-E umsetzen sollen, zu schärfen.

Der Entwurf lässt nach wie vor unklar, was unter dem Begriff der Risikoexposition exakt zu verstehen ist. Auch die weiteren Faktoren, die bei der Auswahl der IT-Sicherheitsmaßnahmen zu berücksichtigen sind, bleiben unklar: das betrifft die Umsetzungskosten, die auch nach geltendem Recht berücksichtigt werden dürfen. Hier hat sich bislang keine klare Rechtsmeinung dazu gebildet, wie dies geschehen darf.

Bei den Aspekten der "gesellschaftlichen und wirtschaftlichen Auswirkungen" bleibt noch immer gänzlich unklar, was darunter zu verstehen ist. Aufgrund der schieren Menge möglicher Einflussfaktoren auf eine nicht definierbare Menge von Aspekten, kann ein alleiniger Kausalzusammenhang jedenfalls augenscheinlich nicht genügen.

TeleTrusT wirbt deshalb dafür, Abs. 1 zu überarbeiten und so zu gestalten, dass er subsumtionsfähig, aber vor allem praktisch anwendbar wird.

In Abs. 2 bleibt unklar, welche Bedeutung den europäischen und internationalen Normen hier zukommen soll. Denn diese beinhalten in der Regel Maßgaben unterhalb des Stands der Technik, also zu den allgemein anerkannten Regeln der Technik. Insoweit erschließt sich keine eigene Wirkung, die über die Verpflichtung, den Stand der Technik zu berücksichtigen, hinausgeht.

TeleTrusT schlägt vor, in Abs. 2 die Fachkreise/Expertenkreise der IT-Sicherheit und deren Empfehlungen (abstrakt) aufzunehmen. Die Fachkreise sind der Ort, wo das Technologieniveau "Stand der Technik" mit konkreten Angaben ausgefüllt wird, vgl. TeleTrusT-Handreichung zum "Stand der Technik in der IT-Sicherheit".

Die Ersetzung des Begriffs der Cyberhygiene durch Sensibilisierungsmaßnahmen muss von einem Abschnitt in der Gesetzesentwurfsbegründung begleitet werden. So wurde die Erklärung zum Begriff der "Cyberhygiene" ersatzlos gestrichen. Die Nennung von "Sensibilisierungsmaßnahmen" bedarf aber ebenfalls einer Konkretisierung. In Art. 17 NIS2UmsuCG-E wird der Begriff zudem noch verwendet, was zu ändern wäre.

Abs. 9: im Rahmen der branchenspezifischen Sicherheitsstandards sollte klargestellt werden, dass sie Angaben darüber zu enthalten haben, wie konkret mit der Aufrechterhaltung des Stands der Technik umgegangen wird. Hier bestand in der Vergangenheit häufig das Missverständnis, ein B3S sei qua definitionem und unbeachtlich konkreter Angaben "als Ganzes" der Stand der Technik. Leider enthalten die im Einsatz befindlichen B3S zu selten Informationen zum Stand der Technik. Das sollte sich ändern.

Die Erweiterung der zu einem Nachweis Verpflichteten auch auf besonders wichtige und wichtige Einrichtungen im Wege einer allgemeinen Rechenschaftspflicht gem. § 30 Abs. 1 a. E. war der Vorschlag von TeleTrusT. Wir halten diese aus mitgeteilten Gründen nach wie vor für wesentlich.

8. § 31 BSIG-E, Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen

Die Anforderungen an IT-Sicherheitsmaßnahmen an Betreiber kritischer Anlagen stellen aufgrund der Relevanz einen wichtigen Regelungskern des BSIG dar. Dennoch bestimmt der § 31 Abs. 1 BSIG-E keinerlei eigenen materiellen Anforderungen, sondern beschränkt den Gesetzesadressaten lediglich bei dessen Beurteilungsspielraum im Rahmen der Maßnahmenauswahl (gem. § 30 BSIG-E). Dies wiederum nur höchst abstrakt. Es bleibt unklar, was "über das Schutzniveau dieser [besonders wichtigen] Einrichtungen hinausgehende Maßnahmen" darstellen. Dies trifft umso mehr zu, je ernster die Gesetzesadressaten den § 30 Abs. 2 S. 1 BSIG-E hinsichtlich der Anforderungen an den Stand der Technik nehmen. Denn wenn die Maßnahmen nach § 30 Abs. 2 S. 1 BSIG-E dem Stand der Technik entsprechen, können diese nicht verbessert werden. Der Stand der Technik selbst bezeichnet bereits die am Markt verfügbaren Bestleistungen von Maßnahmen zur Umsetzung der gesetzlichen Schutzziele.

TeleTrusT hält den § 30 Abs. 1 BSIG-E in der Entwurfsfassung für offensichtlich dysfunktional und rechtlich zu unbestimmt.

Der Zusatz in § 31 Abs. 2, dass sich der Einsatz von Systemen zur Angriffserkennung nur auf diejenigen IT-Systeme, Komponenten und Prozesse bezieht, die für die Funktionsfähigkeit der kritischen Anlagen maßgeblich sind, stellt eine sinnvolle Konkretisierung dar.

9. § 38 BSIG-E, Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

a) "Umsetzungspflicht" für Geschäftsleitungen, § 38 Abs. 1 BSIG-E

§ 38 Abs. 1 BSIG-E sieht weiterhin explizit vor, dass die Geschäftsleitung Risikomanagementmaßnahmen "umsetzen" muss. Nach dem Wortlaut würde eine solche Umsetzungspflicht im Zweifel bedeuten, dass die Geschäftsleitung die Risikomanagementmaßnahmen unmittelbar selbst implementieren muss. Die Aufgabe und Funktion der Geschäftsleitung umfassen naturgemäß die strategische Planung, Leitung und Kontrolle der Unternehmensaktivitäten. In der Praxis wird die Umsetzung der Risikomanagementmaßnahmen daher maßgeblich von den fachlich-technisch Verantwortlichen (z.B. ISB) vorangetrieben.

Die NIS-2-Richtlinie selbst enthält auch keine solche Umsetzungspflicht, sondern ausschließlich eine Pflicht zur "Billigung" und "Überwachung" der Umsetzung. Eine eigene Umsetzungspflicht der Geschäftsleitung besteht im Übrigen auch nicht in den gemäß § 30 Abs. 2 BSIG-E zu berücksichtigenden "europäischen und internationalen Normen", wie etwa der ISO 27001, so dass eine Berücksichtigung ebendieser Normen auf organisatorischer Ebene gerade nicht vollständig erfolgen könnte.

Die Entwurfsbegründung führt dahingehend aus, dass die Geschäftsleitung in Umsetzung dieser Verpflichtung die zu ergreifenden Maßnahmen billigen müssen. Auch nach der Vorgabe 4.2.1 (S. 118) sind Geschäftsleiter zum Billigen und Überwachen verpflichtet. Unklar bleibt damit, warum nicht im Gesetzestext vom "Billigen" gesprochen wird.

Praktisch ist davon auszugehen, dass die Qualität der Risikomanagementmaßnahmen im Unternehmen sinkt, und nicht steigt, wenn die Geschäftsleitung in der jetzigen Entwurfsfassung der Norm verpflichtet wird.

Es sollte daher in § 38 Abs. 1 BSIG-E gemäß den Vorgaben der NIS-2-Richtlinie geregelt werden, dass die Geschäftsleitungen verpflichtet sind, die Umsetzung der nach § 30 zu ergreifenden Risikomanagementmaßnahmen zu billigen und zu überwachen.

b) Überarbeitung der Haftungsregelung, § 38 Abs. 2 BSIG-E

Gemäß § 38 Abs. 2 S. 2 BSIG-E haften Geschäftsleitungen nach "diesem Gesetz" (d. h. dem BSIG-E), wenn die maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelungen nach § 38 Abs. 2 S. 1 BSIG-E enthalten. Das BSIG-E enthält allerdings keine expliziten Haftungsregelungen für Geschäftsleitungen. Die Regelung in § 38 Abs. 2 S. 2 BSIG-E läuft somit ins Leere. Bleiben die aktuellen Regelungen in § 38 Abs. 2 BSIG-E weiter bestehen, sollte aus Gründen der Rechtssicherheit noch eine entsprechende Haftungsregelung aufgenommen werden.

10. § 44 BSIG-E, Vorgaben des Bundesamtes

TeleTrusT begrüßt die Aufnahme des BSI-IT-Grundschutzes in die Mindestanforderungen, die sämtliche Einrichtungen der Bundesverwaltung erfüllen müssen, § 44 Abs. 1 S. 2 BSIG-E. Insbesondere die Aufhebung der Begrenzung der Anwendung des BSI-IT-Grundschutzes auf das Bundeskanzleramt und die Bundesministerien ist sinnvoll, um ein flächendeckendes grundlegendes IT-Sicherheitsniveau bei den Einrichtungen der Bundesverwaltung zu implementieren.

TeleTrusT hebt außerdem hervor, dass eine regelmäßige Evaluierung und Fortentwicklung der Mindestanforderungen entsprechend dem Stand der Technik, wie nach § 44 Abs. 1 S. 6 BSIG-E vorgesehen, absolut unerlässlich ist, insbesondere wenn mit der Umsetzung der Mindestanforderungen nach § 44 Abs. 2 die Erfüllung der Vorgaben nach § 30 gewährleistet sein soll.

11. § 45 BSIG-E, Informationssicherheitsbeauftragte der Einrichtungen der Bundesverwaltung

Im Unterschied zum Informationssicherheitsbeauftragten der Ressorts, der nach § 46 Abs. 2 S. 2 BSIG-E die notwendigen Kenntnisse besitzen muss, kann der Informationssicherheitsbeauftragte dem Wortlaut des § 45 Abs. 2 S. 2 BSIG-E diese noch erwerben. Die Anforderung sollte konsolidiert werden.

12. § 46 BSIG-E, Informationssicherheitsbeauftragte der Ressorts

Hervorzuheben ist die Kompetenz des jeweiligen Informationssicherheitsbeauftragten nach Abs. 4 in begründeten Ausnahmefällen, im Benehmen mit dem oder der jeweiligen IT-Beauftragten des Ressorts den Einsatz bestimmter IT-Produkte in Einrichtungen der Bundesverwaltung innerhalb des jeweiligen Ressorts ganz oder teilweise zu untersagen. Die Begründung des Gesetzes führt hierzu aus, das Veto-

Recht zum Einsatz bestimmter IT-Produkte diene "dem Zweck, bei Bedarf Informationssicherheitsbelange durchsetzen zu können." Worin diese Belange im Einzelnen bestehen, bleibt indes offen.

13. § 47 BSIG-E, Wesentliche Digitalisierungsvorhaben und Kommunikationsinfrastrukturen des Bundes

Begrüßenswert ist der Ansatz, dass bei wesentlichen Digitalisierungsvorhaben Informationssicherheit schon bei der Planung zu berücksichtigen ist, Abs. 5 ("security by design"). Welche Inhalte hier genau zu berücksichtigen sind, bleibt indes offen. Hier empfiehlt sich der Rückgriff auf etablierte Handreichungen wie die zu "Security by Design" von TeleTrusT.

14. § 49 Abs. 3 BSIG-E, Pflicht zum Führen einer Datenbank

Satz 1: Soweit hiernach erforderlich ist, explizit auch "*Überprüfungsverfahren"* zur Verifizierung von Angaben vorzunehmen, kann dies für Domain-Name-Registry-Dienstleister zu Mehraufwand führen. Mit dem Wortlaut der Regelung bleibt unklar, welche konkreten Anforderungen an die Verifizierung der jeweils erfassten Daten gestellt werden.

- Welchen Mindeststandard hat ein Domain-Name-Registry-Dienstleister bei der Verifizierung einzuhalten?
- Darf eine Top Level Domain Name Registry die Freischaltung einer Domain verweigern, wenn ein Domain-Name-Registry-Dienstleister nicht alle Mindestangaben aus § 49 Abs. 2 BSIG-E verifiziert hat?
- Oder, muss die Top Level Domain Name Registry sogleich eigene Anstrengungen zur Verifizierung unternehmen?

Satz 2: Ungenau ist auch, in welchem Umfang und in welcher Tiefe die verlangten *"[…] Vorgaben und Verfahren […]"* öffentlich zugänglich zu machen sind. Reichen dazu Zertifizierungen, Prozessbeschreibungen, Erklärungen/ Selbstverpflichtungen?

15. § 50 BSIG-E, Verpflichtung zur Zugangsgewährung

Die Zugangsgewährungspflicht trifft Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister nur bei begründeten Anträgen. Wann Anträge als begründet zu werten sind, wird in der Begründung zum Entwurf näher beschrieben. Aus Gründen der Bestimmtheit und Rechtsklarheit sollten diese Konkretisierungen Eingang in den Gesetzestext finden.

Die Formulierung des § 50 Abs. 2 leidet unter derselben Ungenauigkeit wie oben zu § 49 Abs. 3 Satz 2 BSIG-E dargestellt. In welchem Umfang und in welcher Tiefe die verlangten "Vorgaben und Verfahren" öffentlich zugänglich zu machen sind, ist offen: Zertifizierungen, Prozessbeschreibungen, Erklärungen/ Selbstverpflichtungen?

16. § 56 Abs. 1 und Abs. 2 BSIG-E, Ermächtigung zum Erlass von Rechtsverordnungen

TeleTrusT begrüßt die stärkere Einbindung von Wirtschaftsverbänden und Vertretern der Wissenschaft bei dem Erlass von Rechtsverordnungen nach Abs. 1 und Abs. 2.

17. § 60 BSIG-E, Zentrale Zuständigkeit in der Europäischen Union für bestimmte Einrichtungsarten

Der Wortlaut von § 60 Abs. 3 und 4 BSIG-E wird zwar fast wortgleich aus der NIS-2-Richtlinie übernommen. Soweit dies aber nicht der Fall ist, werden wichtige Aspekte nicht geregelt. Dies betrifft zum einen die Frage, welche Personen überhaupt als Vertreter agieren dürfen und zum anderen, welche Aufgaben der Vertreter übernimmt. Beide Punkte werden in Art. 6 Nr. 34 der NIS-2-Richtlinie geregelt. Die Formulierung wird diesbezüglich nur in der Begründung zu § 60 Abs. 3 wiedergegeben. Insoweit empfiehlt

es sich aber aus Gründen der Rechtsklarheit, die Definition des Vertreters aus Art. 6 Nr. 34 der NIS-2-Richtlinie entweder in § 2 oder § 60 Abs. 3 BSIG-E auch in den Gesetzestext zu übernehmen.

Auch die Form der Benennung eines Vertreters ist nicht geregelt. Art. 6 Nr. 34 der NIS-2-Richtlinie verlangt eine "ausdrückliche" Benennung des Vertreters. Eine entsprechende Formulierung ist auch hier nur in der Begründung zu § 60 Abs. 3 enthalten. In dem Zusammenhang empfiehlt es sich auch, die Form der Benennung auch dahingehend weiter zu konkretisieren, ob hierfür die Schriftform oder eine andere Form zwingend notwendig ist, um etwaige Unklarheiten zu vermeiden. Die NIS-2-Richtlinie verlangt insofern in Erwägungsgrund 116 eine ausdrückliche *schriftliche* Benennung.

18. § 62 BSIG-E, Aufsichts- und Durchsetzungsmaßnahmen für wichtige Einrichtungen

Es ist weiterhin unklar, wie substantiiert die "Tatsachen" sein müssen, die die Annahme einer nicht oder "nicht richtigen Umsetzung" der Anforderungen aus den §§ 30, 31, 32 BSIG-E, rechtfertigen. Zudem wird eine solche Formulierung gerade nicht in § 61 BSIG-E genutzt. Es ist daher im Zweifel unklar, ob bei der Wahrnehmung der Aufsichts- und Durchsetzungsmaßnahmen gegenüber wichtigen und besonders wichtigen Einrichtungen unterschiedliche materielle Voraussetzungen gelten sollen.

Die Regelung enthält keine Einschränkung dazu, welche Maßnahmen das Bundesamt im Falle der Annahme, dass eine wichtige Einrichtung die Anforderungen aus den §§ 30, 31 und 32 nicht oder nicht richtig umsetzt, ergreifen kann. Dem Bundesamt stünde daher bspw. auch die Möglichkeit offen, von Betreibern wichtiger Einrichtungen nach § 61 Abs. 3 BSIG-E Nachweise zu verlangen. Faktisch bedeutet dies, gerade im Zusammenhang mit den vagen Voraussetzungen des § 62 BSIG-E, eine drastische Ausweitung der Pflichten für wichtige Einrichtungen über den Gesetzeswortlaut hinaus. Es wäre daher wünschenswert, wenn klargestellt wird, welche Maßnahmen in § 61 BSIG-E auf wichtige Einrichtungen angewandt werden können.

19. § 64 BSIG-E, Zuwiderhandlungen durch Institutionen der sozialen Sicherung

§ 64 BSIG-E übernimmt den bisherigen § 14a BSIG fast wortgleich. Entsprechend stellen sich bei § 64 BSIG-E die gleichen Kritikpunkte wie bei dem bisherigen § 14a BSIG.

Es wird weiterhin nicht hinreichend klar festlegt, ob die Anwendbarkeit der dem BSI zustehenden Aufsichts- und Durchsetzungsmittel (siehe §§ 61, 62 BSIG-E) sowie die weiteren Befugnisse des BSI (siehe hierzu etwa die §§ 14 ff. BSIG-E) eingeschränkt werden sollen. Die Ratio der Norm (vgl. § 64 S. 4 BSIG-E) spricht eher für eine entsprechende Sperrwirkung. Ein sachlicher Grund für diese wäre allerdings nicht erkennbar. Es wäre wünschenswert, wenn festgelegt wird, ob und inwieweit das BSI in der Ausübung seiner Befugnisse eingeschränkt werden soll.

20. § 65 BSIG-E, Bußgeldvorschriften

Die Formulierung in § 65 Abs. 8 BSIG-E bedeutet, dass die wichtige oder besonders wichtige Einrichtung nicht zwingend die gesamte zugehörige juristische Person meint, sondern eine solche Einrichtung auch einem "Unternehmen" angehören kann. Dieses Verständnis steht im Widerspruch zum Einrichtungs-Begriff in der NIS-2-Richtlinie (vgl. Art. 3 Nr. 38 NIS-2-Richtlinie). Sofern diese Formulierung auf die Anwendung des unionsrechtlichen Unternehmensbegriffs zurückzuführen ist, wäre eine entsprechende Klarstellung aus Gründen der Rechtsklarheit wünschenswert.